UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE DE ADMINISTRAÇÃO E CIÊNCIAS CONTÁBEIS
CURSO DE BIBLIOTECONOMIA E GESTÃO DE UNIDADES DE INFORMAÇÃO

JOSÉ LUIZ BENTO PIMENTEL JUNIOR

SEGURANÇA DA INFORMAÇÃO: O DESAFIO DO PROFISSIONAL DA INFORMAÇÃO EM RECUPERAR E EXCLUIR DADOS DIGITAIS

RIO DE JANEIRO
2014

JOSÉ LUIZ BENTO PIMENTEL JUNIOR

SEGURANÇA DA INFORMAÇÃO: O DESAFIO DO PROFISSIONAL DA INFORMAÇÃO EM RECUPERAR E EXCLUIR DADOS DIGITAIS

Trabalho de Conclusão de Curso apresentado ao curso de Biblioteconomia e Gestão de Unidades de Informação da Universidade Federal do Rio de Janeiro como requisito para aprovação na disciplina Projeto Final II.

Orientadora: Prof. D. Sc. Maria Irene Fonseca e Sá.

RIO DE JANEIRO
2014

P644s Pimentel JR, J. L. B.

Segurança da Informação: o desafio do profissional da informação em recuperar e excluir dados digitais/ José Luiz Bento Pimentel Junior. – Rio de Janeiro, 2014.

26 f.

Orientadora: Maria Irene Fonseca e Sá;

Trabalho de Conclusão de Curso (Graduação) – Curso de Biblioteconomia e Gestão de Unidades de Informação, Universidade Federal do Rio de Janeiro.

1. Segurança da Informação. 2. Informação digital. 3. Recuperação da Informação. 4. Eliminação da Informação. I. Sá, Maria Irene Fonseca e. II Título.

CDD: 005.8

JOSÉ LUIZ BENTO PIMENTEL JUNIOR

SEGURANÇA DA INFORMAÇÃO: O DESAFIO DO PROFISSIONAL DA INFORMAÇÃO EM RECUPERAR E EXCLUIR DADOS DIGITAIS

Trabalho de Conclusão de Curso apresentado ao curso de Biblioteconomia e Gestão de Unidades de Informação da Universidade Federal do Rio de Janeiro como requisito para aprovação na disciplina Projeto Final II.

BANCA EXAMINADORA

Aprovado em:

Profª Maria Irene Fonseca e Sá
Doutora em Ciência da Informação – IBICT/UFRJ
Orientadora

Prof Nikiforos Joannis Philyppis Junior

Mestre em Economia Empresarial – UCAM

Prof Robson Santos Costa
Mestre em Memoria Social – UFRJ

AGRADECIMENTOS

À professora Maria Irene Fonseca e Sá por ter me orientado na realização deste trabalho.

Aos professores Nikiforos Joannis Philyppis Junior e Robson Santos Costa por terem aceitado participar da banca examinadora.

Aos professores do Curso de Biblioteconomia de Gestão de Unidades de informação, por contribuírem tanto para meu aprendizado e vida profissional.

À Jéssica Serafim, por ter me lembrado de todas as datas e prazos de entrega.

Aos meus amigos, que me apoiaram e me ajudaram quando precisei.

Aos meus familiares, que me deram o suporte que eu precisava.

Aos meus cachorros de estimação, que sempre me animaram ao chegar em casa.

A todos que de alguma forma contribuíram para este trabalho.

“A inteligência, ao contrario do dinheiro ou da saúde, tem esta peculiaridade: quanto mais você a perde, menos dá pela falta dela.”

Olavo de Carvalho

RESUMO

PIMENTEL JR, J. L. B. **Segurança da Informação:** o desafio do profissional da informação em recuperar e excluir dados digitais/José Luiz Bento Pimentel Junior. 2014. 27 f. Trabalho de Conclusão de Curso (graduação). Curso de Biblioteconomia e Gestão de Unidades de Informação. Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2014.

Este trabalho apresenta uma abordagem sobre os aspectos da segurança da informação, no que se compreende dentro deste campo a respeito da recuperação e eliminação de dados armazenados em discos rígidos e outras mídias de armazenamento digital de informação, e sua relação com a profissão do bibliotecário dentro das organizações. Foi realizada uma pesquisa documental onde buscou-se esclarecer o comportamento de dados virtuais mediante aos problemas de eliminação e recuperação, assim como a realização de um comparativo entre diferentes softwares de auxilio nestas tarefas, bem como uma exploração do papel do bibliotecário neste campo, difundido sua importância como profissional da informação dentro das organizações.

Palavras Chave: Segurança da Informação. Informação Digital. Recuperação da Informação. Eliminação da Informação.

SUMÁRIO

1 INTRODUÇÃO

Grandes empresas e organizações trocam seus equipamentos de informática periodicamente a fim de manter seus serviços mais ágeis e os processos informatizados sempre com a melhor tecnologia do mercado. Uma grande organização como a NSA (*National Security Agency* – Agência Nacional de Segurança dos EUA), que afirmou em 2012 ter mais de 30.000 funcionários, trabalha com um grande número de dispositivos de informática, e com isso, um grande número de discos rígidos e diversos outros *hardwares* similares responsáveis por armazenar dados e informações digitais. No momento de realizar a renovação dos equipamentos, estes discos rígidos e mídias de armazenamento são, junto com todo o resto dos computadores e máquinas, "doados" para Korte Lagoon, maior cidade de Ghana, país do continente africano.

Tal material é jogado às toneladas em um local chamado pelos habitantes locais de "Sodoma e Gomorra". O local abriga um imenso depósito de lixo digital, que é catado pelos habitantes mais pobres e depois revendido. O local abriga lixo eletrônico de todo mundo, principalmente no que diz respeito a peças e dispositivos de computadores.

Em 2009, um grupo de jornalistas que estudavam a região para uma matéria sobre o chamado "lixo digital", fez uma alarmante descoberta: por apenas $40 dólares era possível comprar discos rígidos usados por diversas agências governamentais, dentre elas a NSA, NASA (*National Aeronautics and Space Administration* – Administração Nacional de Aeronáutica e Espaço, FBI (*Federal Bureau of Investigation* – Agência Federal de Investigação) e outros diversos órgãos governamentais dos EUA. A situação se tornou desesperadora quando descobriram que era possível recuperar destes discos rígidos dados que deveriam ser confidenciais, inclusive arquivos com conteúdo sigiloso do governo americano, e que isso estava sendo realizado por organizações criminosas ao redor do mundo.

Dessa forma levantamos duas questões, como esses dados, que deveriam ter sido deletados das mídias de armazenamento que foram descartadas conseguem ser recuperados? E mais, que medidas devem ser tomadas para que estes dados sejam definitivamente apagados do disco rígido, impossibilitando a recuperação desses arquivos? Como esse lixo eletrônico deve ser descartado?

Este trabalho realiza uma reflexão sobre diversos trabalhos publicados na área de segurança da informação, tentando se aproximar de uma resposta para estas perguntas, utilizando como plataforma base o Sistema Operacional Windows, da Microsoft. Entretanto, é bom ressaltar que alguns outros sistemas não se diferenciam muito, seguindo princípios similares. Dessa forma, o que será descrito neste trabalho valerá apenas para o Sistema Operacional Windows, contudo, é em muitos pontos semelhante ou idêntico a outros sistemas.

2 JUSTIFICATIVA

Sendo o bibliotecário o profissional responsável pela disseminação e recuperação da informação, é de vital importância que este profissional tenha conhecimento para devidamente armazenar a informação e como propriamente trabalhá-la. Sabemos que em um meio digital, é de extrema importância a utilização dos *backups* (cópias de segurança) para um eventual acidente que cause a perda de dados. Entretanto, e quando o *backup* é perdido, ou quando o *backup* é de uma versão mais antiga da informação que foi perdida, ou até mesmo quando esse backup não existe, quais medidas podem ser usadas para recuperar essa informação que não devia ter sido perdida?

Nos tempos atuais, as empresas e o mercado exigem profissionais da informação que sejam intermediadores da informação interna e externa a organização, o mercado exige, como é dito por Montalli (1997, p. 290),

> [...] bons profissionais de informação capazes de selecionar a enorme gama de variados tipos externos de informação, dispostos em diferentes formatos/fontes de informação, impressos, bases de dados, sistemas *on-line*, instituições, contatos pessoais, *experts* e outros.

Levando estes pontos em consideração, é essencial que o bibliotecário saiba como manipular e utilizar a seu favor os *softwares* e aplicativos do mercado, sabendo se aproveitar das Tecnologias de Informação e Comunicação (TIC's) para evitar eventuais problemas, como a necessidade de recuperar uma informação perdida. Além disso, mostramos como diversas instituições públicas dos EUA sofrem com o vazamento de informações na troca de seus equipamentos. Conseguindo esclarecer medidas e prevenções para estes vazamentos é essencial para o estabelecimento de uma boa atividade profissional.

Ainda falando sobre o profissional da informação, sabemos que, principalmente no meio empresarial e de grande competitividade, muitas das vezes é preciso velar do público uma informação, neste caso, essa informação será privada ou confidencial, podendo ser acessada apenas por alguns. Entretanto, mesmo com um bom sistema de segurança e criptografia, a informação transita por diversos meios de comunicação (seja numa rede como a internet ou uma intranet, ou seja, por *pendrives* e outros dispositivos de armazenamento). Ao transitar por estes meios, essa informação deixa rastros que podem ser recuperados e assim, ocasionar o vazamento de uma informação confidencial à empresa.

Neste trabalho, trataremos também sobre estes rastros e sobre a total remoção de um arquivo ou dado digital, inicialmente abordando até que ponto isso é possível e quais passos devem ser tomados para que a informação possa ser removida de forma definitiva.

3 OBJETIVOS

Este trabalho terá como o objetivo principal:
Identificar a importância do profissional da informação na manutenção da segurança da informação no que diz respeito à recuperação e remoção de dados em meios digitais, mais especificamente nos sistemas operacionais da Microsoft - família Windows.

Para isto, têm-se como objetivos secundários:
Dissertar como a informação e os dados digitais são armazenados em mídias digitais.
Estudar como esses dados podem ser recuperados e removidos.

4 CRIANDO E ARMAZENANDO DADOS DIGITAIS

O Google NGram Viewer é um *software* da empresa Google que oferece um serviço onde é indicada a frequência de uso de uma ou mais palavras especificas em um banco de dados de mais de 5 milhões de livros, publicados entre os anos de 1500 e 2008. Segundo o NGram Viewer, foi a partir de 1980 que a palavra *delete* (do inglês, “deletar”) passou a ser usada com mais frequência que a palavra *erase* (do inglês, “apagar”), na literatura de língua inglesa. O motivo para esta ocorrência é fácil de determinar, bastando ligar a popularização e o avanço das tecnologias e dos computadores que ocorreram a partir desta data. Hoje essa palavra de origem estrangeira é comum em nosso vocabulário.

Porém, como funciona o processo de deletar um arquivo digital? Estamos sempre falando em deletar um arquivo, mas o que acontece quando excluímos uma informação de nossos discos rígidos? Inicialmente precisamos entender como os arquivos são armazenados em um disco rígido, e neste ponto, o sistema funciona da mesma maneira, em qualquer dispositivo, em qualquer sistema operacional, pois aqui falamos do processo físico que ocorre na armazenagem da informação.

Como é dito por Vasconcelos (2007), o disco rígido é composto, basicamente, por um disco magnético e uma agulha de leitura magnética. Quando qualquer tipo de dado digital é salvo no disco rígido do computador, o sistema converte aquele dado em um padrão magnético que fica armazenado no disco. Esse padrão magnético é composto pela ausência ou pela presença de elétrons no disco magnético. Quando o computador precisa recuperar estes dados, a agulha de leitura do Disco Rígido lê este padrão magnético, enviando esta sequência de presença e ausência de elétrons ao sistema operacional ou software instalado em forma de "0" e "1" ("0" representando a ausência de elétrons e "1" a presença). O espaço virtual onde estes bits são armazenados é chamado de *cluster.* O *software* então realiza a interpretação dos dados em forma de bits, trazendo ao dispositivo de saída conectado a informação que estava armazenada.

O processo citado acima é o que ocorre em qualquer Disco Rígido Magnético. O processo se diferencia um pouco nos diferentes tipos de dispositivos de armazenamento (como *pendrives*, CD's/DVD's, cartões de memória, etc), porém ainda assim não é muito diferente, ainda sendo baseado nestes padrões de armazenamento, que tem a principal característica como sendo a ausência e presença de elétrons em sequência.

5 DELETANDO DADOS DIGITAIS

Ao contrário do pensamento de muitos, mesmo após removermos todo o conteúdo de um disco rígido, ou qualquer outra mídia de armazenamento, as informações não desaparecem, elas continuam lá, salvas de forma idêntica como eram anteriormente. Ao deletar um único arquivo seu conjunto sequencial de elétrons não é removido da mídia em que este estava armazenado. O que desaparece é apenas o que chamamos de "apontador".

Quando clicamos em uma pasta no Sistema Operacional (SO) (mais uma vez lembrando, que aqui estamos falando com exclusividade do Windows), o que acontece é que clicamos em um "apontador". Este apontador nada mais é que um recurso visual que nos indica que informação é dentro do ambiente de trabalho do SO. Ao clicar no apontador, realizamos um pedido ao sistema para que a informação referente ao apontador clicado seja recuperada. Quando clicamos em qualquer arquivo do sistema e pressionamos a tecla *delete*, tudo o que fizemos foi remover o apontador. Toda a sequência de elétrons, ou seja, a leitura de bits continua preservada perfeitamente no disco. Como é dito por Malery (2006, p.1) "[...] por causa do jeito que os sistemas operacionais e aplicações funcionam, um arquivo pode ser recuperado e se este arquivo é irrecuperável, a informação contida nele pode ser encontrada em outros arquivos".

Essa informação continuará salva no disco rígido até que ela seja sobrescrita por outra informação, ou seja, mesmo após apagar o apontador e não utilizarmos a informação real que está salva, ela não será excluída, permanecendo salva no disco rígido até que ela precise ser removida para liberar espaço para uma nova informação.

Como foi dito anteriormente, esse recurso de apontadores existe para facilitar a vida dos usuários dos computadores, sendo fortemente ligado à própria utilização do sistema computacional, o grande problema é o mau uso dessas ferramentas. Falamos em ferramentas, pois o sistema operacional tem em sua própria composição uma série de atributos que comprometem a segurança da informação. Essas ferramentas existem com o sentido de agilizar o uso do sistema, contudo elas ao mesmo tempo contribuem para que uma informação torne-se mais recuperável, ou seja, mais difícil de ser eliminada.

O Windows utiliza um espaço no Disco Rígido (HD) chamado de *Swap File* ou *Virtual Space*, que funciona de forma parecida com um relatório de atividades realizadas no sistema. Ele inclui a remoção ou criação de arquivos e pastas, acessos a esses arquivos, páginas da *web* que foram visitadas, e outras informações que ficam armazenadas no HD sem que tenhamos controle ou acesso a elas. É o Sistema Operacional (SO) quem trabalha com as informações do *Swap File*, porém com a utilização de algumas ferramentas é possível acessar estes arquivos e ter acesso a diversas informações que o usuário criou.

Não só o *Swap file* cria esses dados de uso sem a intervenção humana, ou seja, ele cria diversas informações sobre o uso do computador de forma automática, como o sistema operacional ainda tem em seus recursos outras ferramentas que criam outros tipos como as chamadas *Log Files,* ou seja, arquivos com diversas informações de uso. Um exemplo são as chamadas *metadatas* (metadados), que armazenam iniciais de nomes, e nomes completos, utilizados em editores de texto, armazenam também revisões e edições em documentos, mudança de versão em arquivos, entre outras informações. Essas *metadatas* tem função de facilitar o uso do sistema (como auto preencher um nome, ou recuperar um texto editado que foi perdido numa queda de luz).

Existem ainda alguns outros recursos de segurança do sistema operacional, outro exemplo é o Ponto de Restauração. Trata-se de um mecanismo que retorna arquivos do sistema operacional e configurações para um estado anterior ao atual. Dessa forma, quando algum erro é executado, incluindo a remoção acidental de informações, é possível restaurar o sistema para um período anterior a esta remoção, desfazendo o problema e recuperando os arquivos.

Esse método funciona, pois uma vez por dia e a cada grande alteração no sistema operacional, o próprio sistema realiza uma espécie de *backup* de segurança. Esses pontos são criados enquanto houver espaço de armazenamento disponível no disco rígido, sendo após isto pontos de restauração antigos removidos para criar espaço para pontos novos. Também é possível criar pontos de restauração manualmente através do próprio sistema operacional.

Apesar de simples e funcional, esse sistema não apresenta uma função especifica para a recuperação de um único arquivo ou pasta. Dessa forma, caso um único arquivo precise ser recuperado, será necessário restaurar todo o sistema para um ponto anterior, levando muito tempo. Além disso, a cada ponto de restauração criado, mais espaço do disco rígido é consumido, e levando em conta que um ponto de restauração é criado a cada dia e a cada grande alteração no sistema, podemos concluir que é um grande gasto de espaço de armazenamento.

Não devemos pensar que tais ferramentas existem como forma de violar a segurança do usuário. Elas na verdade estão lá para facilitar a vida do usuário, agilizando a recuperação de informações e garantindo a funcionalidade do sistema. Contudo, essas ferramentas podem ser usadas de maneira inadequada por terceiros para a realização de ações inapropriadas.

6 FERRAMENTAS PARA RECUPERAÇÃO DE DADOS

Já falamos aqui dos processos que envolvem a criação e a própria remoção de um arquivo ou dado no meio digital. Já sabemos que esses dados ficam armazenados nas mídias respeitando os padrões binários de bits “0” e “1”, sendo estes padrões interpretados pelo *software* do computador, e já ficou claro entender que estes arquivos podem ser recuperados, já que não são total removidos da sua mídia de armazenamento.

Tendo esses fatores sido explicados, chega aqui o momento de explicar quais são as ferramentas que recuperam esses arquivos até então inexistentes, e como essas ferramentas funcionam.

Primeiramente, existem vários *softwares* no mercado que tem como objetivo a recuperação deste tipo de informação, incluindo *softwares* pagos e outros gratuitos. Neste trabalho iremos fazer uso das ferramentas gratuitas de recuperação.

Também é importante deixar claro que essas ferramentas existem com o princípio de recuperar as informações que foram acidentalmente perdidas. É comum que *pendrives* sejam infectados por vírus de computador, ou até mesmo que um clique acidental, ou um *backup* mal feito possa resultar na perda de uma importante informação, e veremos que algumas ferramentas mais complexas recuperam informações até mesmo de discos rígidos expostos a explosões. É importante olhar para essas ferramentas como *softwares* de ajuda para os usuários.

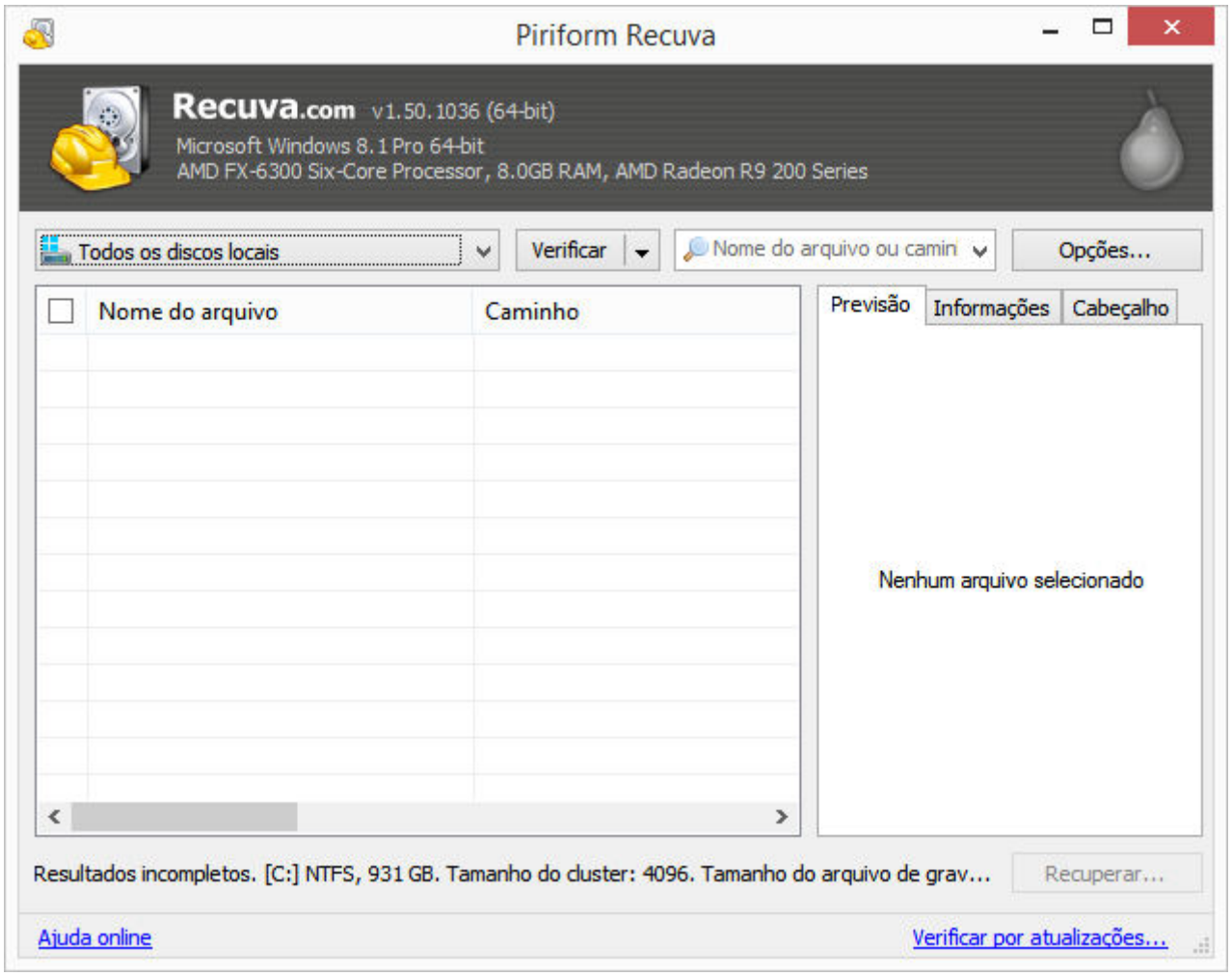
6.1 RECUVA HD

É um *software* gratuito criado pela empresa Piriform, tendo também uma versão paga com mais recursos. Tem uma interface simplista e fácil, de forma a ser facilmente utilizado por usuários de todos os níveis, incluindo inclusive versões em português.

O Recuva HD funciona em três diferentes níveis de recuperação de dados. O primeiro, chamado de “*Regular Recovery Process”* (Processo de Recuperação Regular) escaneia

justamente os arquivos que estão salvos no Disco Rígido, porém que não estão ligados a nenhum apontador. Dessa forma, ele determina quais arquivos foram excluídos e consegue recuperá-los em uma lista, onde o usuário indica quais informações devem receber um novo apontador, sendo assim reutilizáveis normalmente. A Figura 1 a seguir, obtida através de um *print screen* da tela do software, mostra a tela de busca do programa.

Figura 1 – Tela de busca do aplicativo.



O segundo nível, chamado de *"Deep Scan Process"* (Processo de Escaneamento Profundo) utiliza os metadados criados automaticamente pelo sistema, recuperando assim fragmentos de informações dos arquivos. Esse processo é bem mais lento e por recuperar apenas fragmentos, como partes de imagens ou partes de um texto, é praticamente impossível recuperar a informação completa, sendo assim possível apenas a recuperação de parte dela.

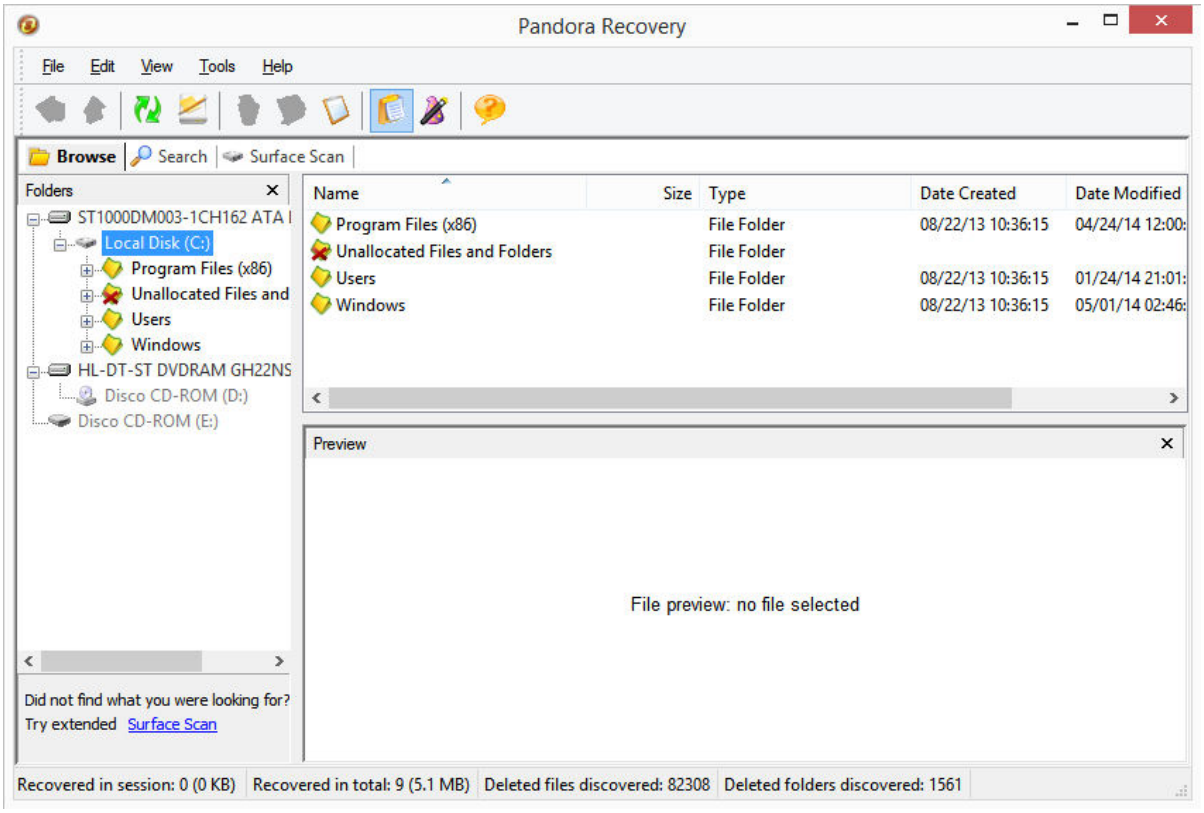
O terceiro e último nível se chama "*Recuvaa's Two-Scan Method*" (Método de Duplo Escaneamento), que como o nome sugere, utiliza os dois outros métodos de recuperação para tentar aumentar as chances de recuperação da informação. Trata-se de um processo ainda mais lento de recuperação, porém com mais chances de obter a informação completa.

6.2 PANDORA RECOVERY

Outro *software* gratuito da empresa Pandora Corp. Diferente do Recuva, o Pandora Recovery tem apenas uma versão em inglês, o que pode dificultar um pouco mais seu uso para usuário leigos na língua. Apesar disso, sua interface ainda é amigável e simples, não requerendo amplo conhecimento para seu uso.

Outro ponto interessante é que este aplicativo apresenta um sistema de navegação pelas pastas do sistema um pouco mais prático que o apresentado pelo Recuva. Enquanto no Recuva o usuário precisa procurar pela pasta especifica que deseja recuperar em uma nova janela, o Pandora permite uma busca pelo próprio aplicativo, como pode ser visto na Figura 2, também obtida através de um *print screen* da tela.

Figura 2 – Sistema de navegação do Pandora Recovery.



Assim como o Recuva HD, o Pandora Recovery funciona de maneira bem parecida, tendo o primeiro e o segundo nível de busca do Recuva HD apenas, não apresentando um sistema de busca conjunto com ambas as ferramentas. Os programas são bem similares e por isso não existem muitos pontos de diferença a serem levantados.

7 FERRAMENTAS PARA REMOÇÃO SEGURA DE DADOS

Assim como os *softwares* de recuperação de dados existentes no mercado, temos *softwares* para tornar a recuperação desses dados ainda mais difícil, ou até mesmo teoricamente impossível. Na verdade, veremos aqui que para tornar tal recuperação mais próxima do impossível, é bem mais recomendável a utilização de recursos físicos que digitais.

Tratando do meio digital, sabemos que a informação é armazenada em bits na forma de “0” e “1”, numa sequência binária. O que esses *softwares* de segurança fazem é modificar de forma aleatória essa sequência de bits, de forma que todo o arquivo se torne corrompido e irrecuperável.

Além disso, é comum que esses *softwares* sobrescrevam o espaço onde está alocada a informação. Sendo assim, se temos uma informação salva em um determinado espaço do disco rígido, o *software* substitui essa informação diversas vezes por uma sequência de bits aleatória, fazendo com que a informação principal seja sobrescrita diversas vezes, tornando-se inutilizável. Quanto maior o número de sobrescrições, mais lento e mais seguro é a total eliminação da informação.

7.1 METODOS FISICOS DE ELIMINAÇÃO

A total eliminação de uma informação do meio digital é praticamente impossível, mesmo utilizando os mais modernos *softwares*. É quase impossível assegurar que todos os vestígios de um arquivo ou informação foram eliminados. Sendo assim, é comum que algumas organizações adotem uma medida mais radical para a eliminação segura da informação de seus discos rígidos.

Esses métodos são mais definitivos, pois ao invés de ter como maior preocupação a eliminação digital, eles se preocupam em eliminar fisicamente a mídia em que a informação está armazenada. A maior preocupação está no fato de que, digitalmente falando, nenhuma

informação pode ser eliminada de forma definitiva, nunca há a garantia de que aquela informação não será recuperada. É por isso que Malery (2006, p.7) diz que

> De uma perspectiva coorporativa, um individuo deverá determinar o valor da informação e determinar os passos que poderão ser considerados "razoáveis e práticos" para prevenir que a informação privada seja roubada ou recuperada por competidores ou outros grupos que tem a intenção de realizar espionagem coorporativa. A pergunta se torna então quantas vezes essa informação deverá ser sobrescrita?

Com isso, muitas organizações tomam medidas físicas para a eliminação da informação. O Departamento de Defesa da Marinha dos EUA indica que seu procedimento padrão para eliminação de discos rígidos e outras mídias de armazenamento é, basicamente, sobrescrever cada bit de forma aleatória, e em cima de nova sequência aleatória, novamente sobrescrever os bits com outra sequência aleatória, repetindo este processo por um total de treze vezes, tomando o devido cuidado de sobrescrever inclusive os *clusters* que não foram utilizados. Depois deste processo, o disco de armazenamento é exposto à um *degausser* (aparelho que expõem objetos a intensos campos eletromagnéticos, "desmagnetizando" o objeto) por duas vezes seguidas, para então ser destruído, sendo fisicamente derretido ou triturado e prensado com outros metais.

Obviamente, o método acima que é utilizado pela marinha e aeronáutica dos EUA é bem mais definitivo que a maior parte dos métodos utilizados, contudo tem um custo de recursos e de tempo quase inconcebível para a maior parte das organizações.

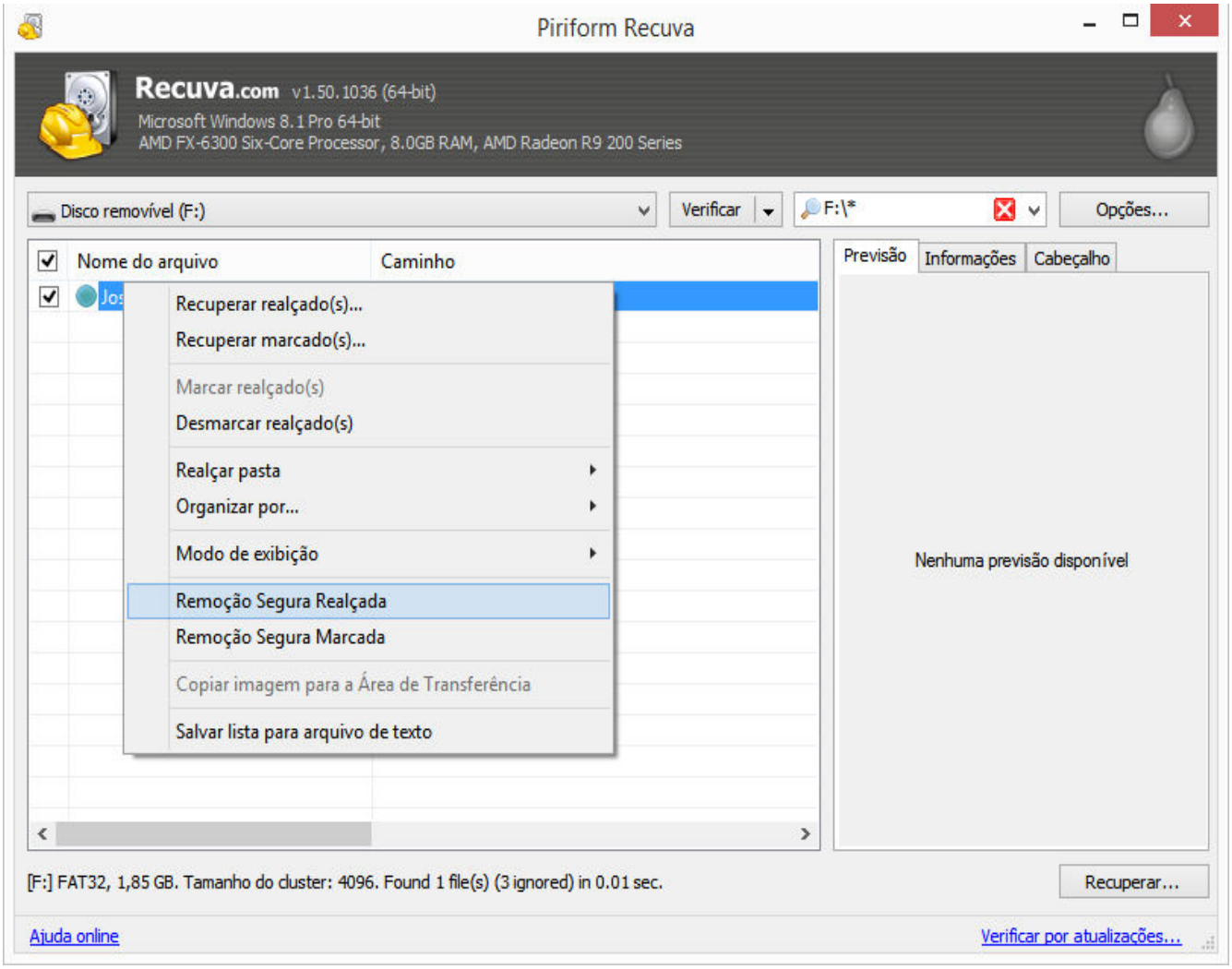
Como métodos de menores proporções são utilizados apenas os mecanismos digitais de remoção de dados, ou seja, *softwares* de remoção de dados, que iremos ver a seguir. Apesar de não tão definitivos, eles são mais viáveis. Não podemos nos esquecer de manter medidas "razoáveis e práticas".

7.2 RECUVA HD

Mais uma vez recorremos a esse *software* que da mesma forma como consegue recuperar uma informação, inclui também ferramentas para tornar essa informação irrecuperável. Ele funciona através de sobrescrição de dados, sobrescrevendo o espaço do disco rígido diversas

vezes com bits aleatórios, como já foi dito. A seguir temos a Figura 3, obtida por um *print screen* do programa, mostrando a opção de remoção segura do aplicativo

Figura 3 – Opção de Remoção Segura do Recuva.



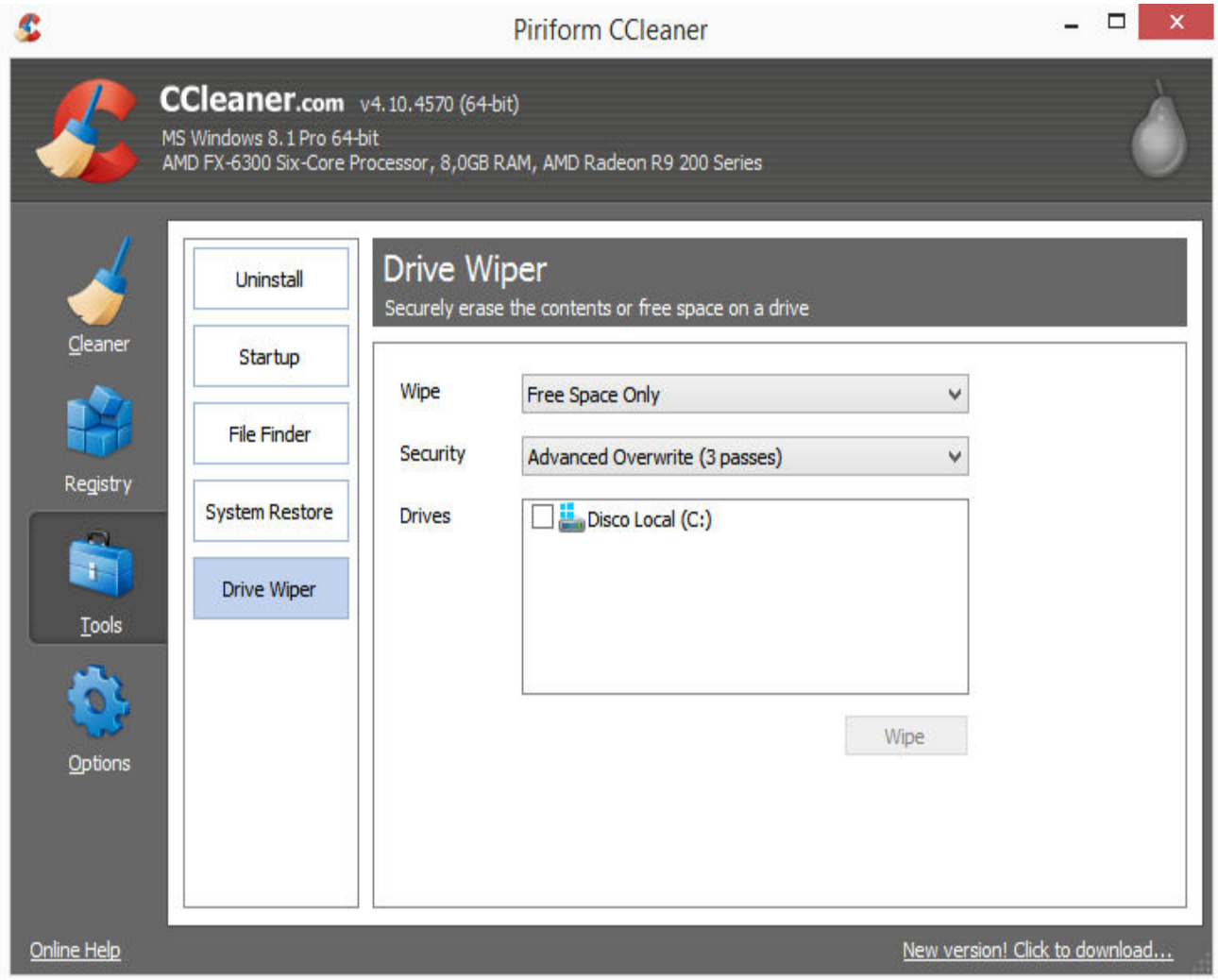
Um ponto interessante dessa funcionalidade do Recuva, é que ele primeiramente identifica o dado a ser excluído e todos os metadados ligados a ele e então os sobrescreve. Isso agiliza o processo, entretanto, não existe garantia que ele conseguirá capturar todos os fragmentos da informação a ser deletada de forma definitiva, podendo apresentar falhas e deixar vestígios.

7.3 CCLEANER

Software da mesma empresa criadora do Recuva HD, entretanto com um funcionamento diferente. Seu método de sobrescrição e identificação dos dados a serem deletados é diferente, apesar de a interface sugerir que o processo é o mesmo. Diferentemente do Recuva, o

CCleaner não utiliza um sistema de busca individual para deletar os arquivos, ele realiza a eliminação de todos os dados da mídia, como mostrado na Figura 4 obtida por um *print screen.*

Figura 4 – Exemplo da tela de sobrescrição do aplicativo.



Na verdade, o CCleaner apresenta uma ferramenta de pesquisa parecida com a do Recuva HD, onde ele busca todos os espaços e informações armazenadas que não apresentem apontadores. Após isso, ele exclui todos esses dados, ou seja, sua forma de remoção de arquivos é mais generalizada, contudo ele apresenta a opção de sobrescrever o arquivo por mais vezes, oferecendo maior segurança.

8 METODOLOGIA

Este trabalho foi realizado através de pesquisa bibliográfica do tema segurança da informação, em trabalhos relacionados, envolvendo: periódicos, livros e artigos acadêmicos. Acompanhando a pesquisa bibliográfica, foi realizado também um experimento de testes, em pequenas proporções, para o levantamento da qualidade dos *softwares* que estão sendo apontados neste trabalho.

Em uma tentativa de esclarecer o uso e a qualidade dos *softwares* citados neste trabalho, foram realizados testes utilizando as devidas funções dos *softwares,* testando suas capacidades e o quão bem eles conseguem cumprir seus objetivos, sejam eles excluir um arquivo ou recuperá-lo. Foram utilizadas as ferramentas principais trabalhadas até então, que seriam o "Recuva HD", "Ccleaner" e o "Pandora Recovery".

Inicialmente, foi utilizada um *pendrive* mídia de armazenamento nova, que nunca havia sido usada, para evitar que antigos arquivos pudessem entrar em qualquer tipo de conflito ou influenciar os resultados. Nessa mídia, foram armazenadas duas fotos idênticas, porém em diferentes formatos, já que o tamanho do arquivo e o tipo podem ser fatores de influência nos testes. Além disso, foram armazenados também dois arquivos de texto, no formato .doc e .pdf, ambos por serem bastante utilizados na atualidade.

Os arquivos foram então excluídos da mídia, e então foram utilizadas as ferramentas mencionadas para tentar recuperá-los. Após foram analisados os resultados obtidos, avaliando a velocidade, e se os arquivos foram recuperados em sua integridade.

Após este passo, foram utilizadas as ferramentas de sobrescrição para tentar limpar a mídia de armazenamento de forma mais definitiva dos arquivos, e assim reutilizar as ferramentas de recuperação, e novamente, avaliar os resultados obtidos, realizando uma análise da funcionalidade de cada um dos *softwares* utilizados.

9 RESULTADOS

O primeiro teste foi realizado com o "Recuva HD", que se mostrou muito eficiente. Recuperou rapidamente todos os arquivos com total integridade, sem mostrar nenhum tipo de falha nos documentos de texto ou imagens. Em seguida, foi utilizado o "Pandora Recovery", que conseguiu apresentar o mesmo êxito, e tempo de recuperação praticamente idêntico.

Contudo, o “Pandora Recovery” apresenta uma interface um pouco menos amigável, o que poderá ser problemática para usuários menos experientes.

Em um segundo momento, foi utilizado o “Recuva HD” para eliminar os arquivos desta mídia. O processo se mostrou rápido, realizado quase que instantaneamente, mas ao reutilizar o “Recuva HD” para tentar recuperar estes arquivos excluídos, notamos na própria ferramenta que ela consegue recuperar os nomes dos arquivos que estavam ali. Mais ainda, ao utilizar esta ferramenta para excluir e sobrescrever os arquivos, ela cria um arquivo de formato desconhecido, porém que possivelmente contém informações sobre as informações que foram sobrescritas.

Contudo, os arquivos de imagem e texto que inicialmente estavam gravados estavam irrecuperáveis. Entretanto, ainda era possível ver o nome que estes arquivos tinham quando existiam e ainda, a criação de um arquivo oculto desconhecido. Sendo assim, apesar de ser uma boa ferramenta para recuperar informações perdidas, o “Recuva HD” apresenta diversas falhas em tornar informações irrecuperáveis.

O “Pandora Recovery” não foi capaz de recuperar os arquivos sobrescritos anteriormente, mas ainda foi capaz de identificar o nome dos arquivos que existiam antes, reforçando a falha do “Recuva HD”.

O próximo passo contava então em utilizar o “Ccleaner” para limpar a mídia de armazenamento. Um fato interessante desta ferramenta é que ela conta com diversas opções de sobrescrição, podendo sobrescrever o mesmo *cluster* de armazenamento do arquivo até trinta e duas vezes, contudo, quando maior o número de sobrescrições, mais tempo o processo leva. Utilizamos a opção de sobrescrever três vezes.

Todo o processo demorou cerca de vinte minutos, mostrando que esta medida pode ser demorada. Isso se deve ao fato de que o “Ccleaner” sobrescreve cada espaço na mídia, e não apenas os espaços usados. Apesar da longa espera, esta ferramenta se mostrou bem definitiva, e apenas com a sobrescrição realizada em três vezes consecutivas foi suficiente para tornar a mídia livre de qualquer vestígio que os outros *softwares* pudessem detectar.

É claro, não é possível afirmar que o "Ccleaner" seria uma ferramenta de limpeza definitiva, já que existem outros métodos e outras ferramentas muito mais sofisticadas, contudo, em um nível local ele se mostrou a ferramenta mais eficiente.

10 O BIBLIOTECÁRIO NA SEGURANÇA DA INFORMAÇÃO

O mundo vem passando por diversas transformações, principalmente tecnológicas, que influenciam de maneira direta a forma de se viver da sociedade e principalmente os meios de comunicação das organizações. As novas tecnologias tem como principal objetivo facilitar o trabalho e ampliar a funcionalidade das organizações, em geral, melhorando o cotidiano. Segundo Tarapanoff (2006, p. 9),

> O contexto que se impõe sobre as corporações hoje é o da sociedade da informação e do conhecimento. Esta nova sociedade, globalizada, apoia-se em tecnologias de informação e comunicação, exigindo, para que esta última ocorra, uma estrutura em rede.

Entretanto, não são incomuns os casos em que as tecnologias são usadas de maneiras inapropriadas, muitas vezes até ilegais, ou então as próprias ferramentas que nos são proporcionadas permitem aberturas e acessos indesejados ao espaço privado. Já mostramos essas influências, e até aqui este trabalho realizou uma abordagem sobre este tema, ligado à segurança da informação.

Assim, constantemente estamos expondo informações privadas a uma vulnerabilidade, principalmente dentro dos meios de processamento das organizações, meios estes em que as TIC's são de uso constante. Sendo assim, é importante a presença de uma política de segurança, onde os métodos até aqui mencionados sejam implantados e estabelecidos de forma a prevenir eventuais problemas informacionais.

Esta política seria um conjunto de normas e regulamentos criados para orientar gestores de sistemas empresariais, regulando como a organização gerencia e protege suas informações. Sendo assim, essa política irá se referir a três figuras: a) o usuário ou profissional que irá participar de todo este sistema; b) a organização e a informação trabalhada por ela; c) o ambiente em que todo o sistema se insere.

Isso significa que a política precisa ser criada de forma que ela atenda às necessidades de proteção e gerenciamento da organização, devendo suportar as limitações e responsabilidades dos seus usuários e profissionais e compreender as novas tendências de mercado, tecnologias e principalmente observar aspectos de competitividade.
O profissional designado para desenvolver e manter essa política precisa saber trabalhar a informação em todos os seus processos, sendo também um profissional responsável em entender necessidades e demandas de usuários ou organizações, tendo de saber analisar criticamente o ambiente em que está inserido.

O bibliotecário, o analista de sistemas, o gestor ou administrador são profissionais capazes de compreender estas necessidades, ainda que seja desejável uma equipe multidisciplinar para tal.

O bibliotecário será capaz de atuar nessa equipe, pois sua formação atende todas as necessidades listadas, ele é capaz de gerenciar todo um sistema de informação e criar uma política de segurança. Como é dito por Corrêa e Pereira (2013, p.6),

> "O bibliotecário está em busca de uma identidade expansiva, interdisciplinar e "aberta" às diversas áreas do conhecimento, utilizando-se das tecnologias de comunicação e informação, tornando-se agente corresponsável pelos processos de tomada de decisão nas organizações."

Uma pesquisa realizada por Corrêa e Pereira (2013), em um trabalho intitulado "Competências do bibliotecário no desenvolvimento e implementação de políticas e normas de segurança da informação", teve como objetivo identificar nos profissionais de biblioteconomia este perfil voltado para a criação de políticas e manutenção da segurança da informação em diferentes unidades de informação, em Florianópolis (SC).

Tratou-se de uma pesquisa feita através de um questionário distribuído por diversas instituições privadas da cidade, sendo respondido por um total de oito bibliotecários. Destes participantes, um total de três trabalhavam diretamente com a segurança da informação das instituições a qual pertenciam, e os restantes que não trabalhavam diretamente com a segurança da informação afirmaram que reconhecem a importância do profissional nesta área.

Verificou-se também que os bibliotecários participantes da pesquisa tinham conhecimento de normas internacionais de segurança da informação, tendo assim total capacidade para atuarem na área, sendo capazes de trabalhar na criação de políticas de segurança. Apesar de não mostrar um número, a pesquisa disse ter tido também a participação de profissionais de TI que, apesar de não serem bibliotecários, afirmaram reconhecer a importância deste profissional na área. Esse dado mostra o reconhecimento que o profissional bibliotecário tem obtido ao longo do tempo na sociedade.

11 CONSIDERAÇÕES

Sendo assim, é preciso afirmar primeiramente que a total remoção de uma informação de uma mídia digital é praticamente impossível, visto que o sistema computacional está sempre tentando agilizar nosso trabalho através do armazenamento de informações de segurança e de recuperação mais prática da informação. É importante ver que estas medidas existem para ajudar o usuário, e tornar toda a utilização do computador uma tarefa mais prática.

Sendo essa remoção de informações quase impossível de ser feita por completo, é preciso que as organizações tenham uma boa política de segurança e profissionais capazes de manter e atualizar essa política, preservando assim a integridade e a privacidade das informações da empresa, tendo sempre em mente a utilização de métodos “razoáveis e práticos”. Não podemos ignorar também a importância das ferramentas citadas para a recuperação de dados removidos, já que estas podem solucionar diversos problemas de recuperação em caso da perda acidental de informações.

Sabendo da existência dessas ferramentas, é preciso tomar cada vez mais cuidado com as informações que criamos e como as utilizamos, tomando os devidos cuidados para que não possam ser utilizadas contra nós. Vemos que o bibliotecário tem grande importância nesse sentido, já que diversas organizações sofrem com esse problema na segurança da informação e que com o devido conhecimento de utilização das ferramentas é possível prevenir diversos vazamentos informacionais e preservar a integridade informacional. Mostramos que o bibliotecário é um profissional totalmente capaz de atuar na área de segurança e que o cenário empresarial vem aceitando cada vez mais a figura desse profissional na área.

REFERÊNCIAS

BLATTMAN U, FACHIN G R B, RADOS, G J V. **Bibliotecário Na Posição Do Arquiteto Da Informação Em Ambiente Web.** Disponível em: <http://www.ced.ufsc.br/~ursula/papers/arquinfo.html>. Acesso em: 25 mar. 2014.

CORRÊA, A. C. R, PEREIRA, A. M. Competências do bibliotecário no desenvolvimento e implementação de políticas e normas de segurança da informação**. XXV Congresso Brasileiro de Biblioteconomia, Documento e Ciência da Informação** – Florianópolis, SC, Brasil, 07 a 10 de julho de 2013.

CRETH, S. D. **The Electronic Library: Slouching Toward the Future or Creating a New Information Environment.** Disponível em: <http://www.ukoln.ac.uk/services/papers/follett/creth/paper.html>. Acesso em: 25 mar. 2014.

DOCTOROW, C. **Illegal e-waste dumped in Ghana includes unencrypted hard drives full of US security secrets.** Disponível em: <http://boingboing.net/2009/06/25/illegal-e-waste-dump.html>. Acesso em: 24 nov. 2013.

FREITAS, A. R. **Pericia Forense Aplicada à informática**. São Paulo: IBPI, 2003. Disponível em: <http://www.ebah.com.br/content/ABAAAAbjUAJ/pericia-forense-aplicada-a-informatica>. Acesso em: 25 mar. 2014.

Google Ngram Viewer. Disponível em: <https://books.google.com/ngrams>. Acesso em: 24 nov. 2013;

GUTMANN, P. Secure Deletion of Data from Magnetic and Solid-State Memory. The Sixth USENIX Security Symposium, July 22–25, 1996, San Jose, California, EUA.

KLEIN, P. **Ghana: Digital Dumping Ground**. Inglaterra: PBS, 2009. Disponível em <http://www.pbs.org/frontlineworld/stories/ghana804/video/video_index.html>. Acesso em: 24 nov. 2013.

MALLERY, J. R. **Secure File Deletion: Fact or Fiction?** Maryland: SANS, 2006.

MICROSOFT: **Windows Support**. Disponível em: <http://windows.microsoft.com/pt-BR/windows-vista/System-Restore-frequently-asked-questions>. Acesso em: 24 nov. 2013.

MONTALLI, K. M. L. Perfil do profissional de informação tecnológica e empresarial. **Rev. Ci. Inf., Brasília**, v. 26, n. 3, p. 290-295, set/dez. 1997.

NASCIMENTO, J. S.; JERÔNIMO, K. S.; SEGUNDO, P. C. S. **Análise de Ferramentas Forenses de Recuperação de Dados.** Brasília: IOFCS, 2010.

PIRIFORM. **How Recuva Works.** Disponível em: <http://www.piriform.com/docs/recuva/technical-information/how-recuva-works>. Acesso em: 24 nov. 2013.

TARAPANOFF K, ARAUJO R H, CORMIER, P M J. Sociedade da informação e inteligência em unidades de informação. **Rev. Ci. Inf., Brasília**, v. 29, n. 3, p. 91-100, set./dez. 2000.

VASCONCELOS, L. **Hardware na prática.** Rio de Janeiro: [s.n.], 2007.